

CLAIMS

What is claimed is:

- 5 1. A method for generating a query comprising the steps of:
 - a) receiving a cookie that includes an encrypted buffer that includes a profile code that indicates the services that a user is entitled to use, said profile code encrypted using an encryption key generated using a first seed component, a second seed component and a third seed component, said first seed component further comprising user identification data, said cookie also including said a second seed component and said third seed component, said second seed component and said third seed component not encrypted;
 - b) generating a request buffer that indicates a desired service;
 - c) receiving said user identification data from a user;
 - 15 d) encrypting said request buffer using said second seed component as an encryption key so as to form an encrypted portion of a query; and
 - e) generating a query that comprises said user identification data received in step c) and that includes said encrypted portion of said query, said query also including said third seed component and said encrypted buffer, said third seed component and said user identification data received in step c) not encrypted.
2. A method as recited in Claim 1 further comprising the step of:
 - f) transmitting said query to an authentication server.

3. A method as recited in Claim 2 further including the steps of:
g) receiving a response from said authentication server.

5 4. A method as recited in Claim 3 wherein the response received in step
g) is encrypted using said second seed component as an encryption key.

10 5. A method as recited in Claim 1 wherein said user identification data is
numerical and wherein said third seed component further comprises a
randomly generated number.

15 6. A method as recited in Claim 5 wherein said encryption key is
determined using a hash of at least three elements.

20 7. A method as recited in Claim 6 wherein said encryption key is
determined by a MD-5 hash of said first seed component, said second seed
component and said third seed component.

8. A method as recited in Claim 6 wherein said encrypted buffer is further
encrypted using said second seed component.

9. A computer system comprising:

a processor coupled to a bus;

a memory unit coupled to said bus and comprising instructions that when executed by said processor implement a method for generating a query

5 comprising the steps of:

a) receiving a cookie that includes an encrypted buffer that includes a profile code that indicates the services that a user is entitled to use, said profile code encrypted using an encryption key generated using a first seed component, a second seed component and a third seed component, said first

10 seed component further comprising user identification data, said cookie also including said a second seed component and said third seed component, said second seed component and said third seed component not encrypted;

b) generating a request buffer that indicates a desired service;

c) receiving said user identification data from a user;

15 d) encrypting said request buffer using said second seed component as an encryption key so as to form an encrypted portion of a query; and

e) generating a query that comprises said user identification data received in step c) and that includes said encrypted portion of said query, said query also including said third seed component and said encrypted buffer, said 20 third seed component and said user identification data received in step c) not encrypted.

10. A computer system as recited in Claim 9 wherein said method further comprises the step of:

f) transmitting said query to an authentication server.

11. A computer system as recited in Claim 10 wherein said method further comprises the step of:

5 g) receiving a response from said authentication server.

12. A computer system as recited in Claim 11 wherein the response received in step g) is encrypted using said second seed component.

10 13. A computer system as recited in Claim 9 wherein said user identification data is numerical and wherein said third seed component is a randomly generated number.

14. A computer system as recited in Claim 9 wherein said encryption key
15 is determined using a hash of at least three elements.

15. A computer system as recited in Claim 14 wherein said encryption key is determined using a MD-5 hash of said first seed component, said second key component, and said third seed component.

20 16. A computer system as recited in Claim 14 wherein said computer system further comprises a palmtop computer.

17. A method for generating a query from a palmtop computer comprising:

a) providing user identification data to a user, said user identification data comprising a first seed component of three seed components used for

5 generating an encryption key;

b) receiving a cookie that includes a second seed component and a third seed component of said three seed components used to generate said encryption key, said cookie also including an encrypted buffer encrypted using said encryption key;

10 c) generating a request buffer that indicates a desired service;

d) receiving said user identification data from a user;

e) encrypting said request buffer using said second seed component as an encryption key so as to form an encrypted portion of a query; and

f) generating a query that comprises said user identification data

15 received in step d) and that includes said encrypted portion of said query, said query also including said third seed component and said encrypted buffer, said third seed component and said user identification data received in step d) not encrypted.

20 18. A computer system as recited in Claim 17 wherein said method further comprises the step of:

g) transmitting said query.

19. The method of Claim 18 further comprising the steps of:

h) receiving a response.

20. The method of Claim 17 wherein said encryption key is determined using a MD-5 hash of said first seed component, said second key component,
5 and said third seed component.

00000000000000000000000000000000